REMARKS

In accordance with the foregoing, claims 1 and 8 are amended. Claims 1-19 are pending and under consideration. No new matter is presented in any of the foregoing and, accordingly, approval and entry of the amended claims are respectfully requested.

ENTRY OF AMENDMENT UNDER 37 CFR §1.116

Applicant requests entry of this Rule 116 Response because it is believed that the amendment of claims 1 and 8 puts this application into condition for allowance and should not entail any further search by the Examiner since no new features are being added or no new issues are being raised

REQUEST TO WITHDRAW CURRENT OFFICE ACTION AS INCOMPLETE

The current Office Action does not provide any response to the Applicant's arguments filed April 5 2004 traversing the rejections of claims 3-7 filed in the previous Office Action. However, the current Office Action repeats the Examiner's contentions in the final rejection of claims 3-7, and applies the contentions in the rejections of claims 13-15 and 18-19. (Action at pages 6-7).

As set forth in MPEP §707.07(f) entitled Answer All Material Traversed "an examiner must provide clear explanations of all actions taken by the examiner during prosecution of an application."

Applicant submits that the current Office Action is incomplete and the finality should be withdrawn, the office action reissued with a new response date since the Examiner has not responded to the previously filed arguments.

ART RELIED ON BY EXAMINER IS NONANALOGOUS ART

As understood in the art, a finite field is defined as a field which the number of element is p^m may be expressed by the prime number p and a m-th order irreducible polynomial. In expressing a finite field, it is necessary to assign a prime number for a p and a m-th order irreducible polynomial (m being 2 or more). According to aspects of the present invention, a pair of a prime number p and m-th order irreducible polynomials is automatically generated only if a user specifies a bit length corresponding to the value, p^m (or obtained from a table).

The Examiner mistakenly contends there is an equivalence between the cited art and the present invention in terms of "random number generation" or "random polynomial generation." According to aspects of the present invention, however, data is generated representing a finite field (a pair of a prime number, which is not a number picked up in random and an irreducible

polynomial that not a polynomial picked up in random) that complies to any size a user may specify.

PAGES 2-7: REJECTION OF CLAIMS 1-3, 6-12 AND 14-19

Independent claim 1, as amended, recites a data generating apparatus including "inputting a condition specified by a user for designating a finite field corresponding to a mathematical finite aggregate in which four arithmetical operations are defined, (and) a generation device automatically generating expression data of the finite field based on the inputted condition; and an expression data storage device storing the generated expression data."

Independent claim 8, as amended, recites a medium on which is recorded a program enabling a computer to execute a process "specifying a condition automatically generating expression data of a finite field corresponding to a mathematical finite aggregate in which four arithmetical operations are defined."

Independent claim 9 recites a method including "designating a condition for designating a finite field . . .(and) automatically generating expression data of the finite field based on the designated condition."

Independent claim 10 recites an apparatus including "inputting means for inputting a condition for designating a finite field . . . (and) generating means for automatically generating expression data of the finite field based on the inputted condition." Independent claim 11 recites an apparatus including " inputting a condition designating a finite field; and an expression data storage device storing expression data of the finite field, wherein the expression data is based on the inputted condition."

The Action concedes that Leppek does not teach "details that would indicate that the PGP algorithm whose conditions are of a finite field corresponding to a mathematical finite aggregate in which four arithmetical operations are defined, a number of elements of the finite aggregate being expressed as p^m with p and m as prime number and a positive integer indicating an extension degree, respectively." (Action at pages 3 and 4).

Nevertheless the current Office Action rejects independent claims 1, 6, 8-11, and 16 (and respective dependent claims 2-3, claim 7, claim 12, claims 14-15, and claims 17-19) under §103(a) over Leppek in view of Schneier (Applied Cryptography, 1996, pages 584 and 320).

The Examiner contends that since Leppek teaches a system that uses PGP, and Schneier teaches details of a PGP algorithm, it would have been obvious to modify Leppek with Schneier

to provide "the details." (Action at page 3).

Leppek Does Not Teach Generating Expression Data Of A Finite Field

Applicant submits that Leppek is nonanalogous art, and the cited art alone or in combination does not teach generating any finite field expression data.

As understood in the art, a finite field is strictly defined as "a field which has a finite number q of elements in it." (See, for example, Neal Koblitz A Course In Number Theory and Cryptography, Second Edition at pages 33, Springer-Verlag, New York 1991.)" Koblitz further defines (page 31) that a field, as understood in the art,

> . . . is a set F with a multiplication and addition operation which satisfy the familiar rules -associativity and commutativity of both addition and multiplication, the distributive law, existence of an additive identity 0 and a multiplicative identity 1, additive inverses, and multiplicative inverses for everything except 0. The following examples of fields are basic in many areas of mathematics: (1) the field Q consisting of all rational numbers; (the filed R of real numbers; (3) the field C of complex numbers ; (4) the field Z/pZ of integers modulo a prime number p.

Applicant submits that as strictly defined in the art cited art alone or in combination does not teach generating any finite field expression data.

The Examiner also contends that Schneier:

> discloses the details of the PGP algorithm (page 584), which includes IDEA. The IDEA algorithm has S-boxes which have the condition are of a finite field corresponding to a mathematical finite aggregate in which four arithmetical operations are defined, a number of elements of the finite aggregate being expressed as p^m with p and m as prime number and a positive integer indicating an extension degree, respectively (page 320 paragraph 2).

(Action at page 4).

Applicant submits that the Examiner is mistaken in this contention and that with respect to the three operations taught by Schneier on page 320, paragraph 2, XOR and addition modulo $2^{16} + 1$ have nothing to do with the finite field operations, whatsoever.

Arguendo the operation "multiplication modulo $2^{16} + 1$" could be regarded as a multiplication operation within a finite field because $2^{16}+1$ happens to give a prime number. However, the chance that an IDEA algorithm contains an operation that may be regarded as an operation within a finite field among the plurality of various operations the IDEA algorithm contains merely because a prime number is a constant, e.g., fixed to $p = 2^{16} + 1$.

Applicant submits that such a chance occurrence as taught by Schneier does not teach features as recited by claims of the present invention, in which, in response to an input for specifying a bit length, a finite field expression is returned by extracting a prime number that is expressed in this specified bit length from a table or by generating a prime number having this

specified bit length.

Further, since in a case of the IDEA algorithm as taught by Schneier, an *arguendo* "finite field" is unchangeable, Applicant submits that the proposed combination by the Examiner teaches away from recited features, using claim 1 as an example, of "inputting a condition for designating a finite field" or "automatically generating expression data of the finite field based on the inputted condition."

No Motivation To Combine The Teachings Of The Art

The Examiner contends that the motivation to modify Leppek with Schneier is because "Leppek does not disclose the details ... while Schneier gives the details." (Action at pages 3 and 4). As set forth in MPEP 2142 "there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings." Applicant submits that the Examiner's contention does not meet such standards.

Further, dependent claims recite features not taught by the cited art, alone or in combination. For example, dependent claim 2 recites an apparatus including "an operation device performing a finite field operation based on the expression data stored in said expression data storage device." Even assuming *arguendo*, Schneier teaches data of a finite field expression, such data is unchangeable and does not teach data representing "a finite field operation based on the expression data" that corresponds to a specified bit length.

Dependent claim 3 recites an apparatus "wherein when a bit length of the prime number is inputted as the condition, said generation device automatically generates prime number data corresponding to the bit length and stores the generated prime number data in said expression data storage device."

The Examiner contends (page 3) that "the size of the keys is a design choice it is possible to select a length of an RSA key."

Applicant submits, however, that as understood in the art an RSA key includes a part constituted by a compound number, and consequently is not a prime number as an expression of a finite field. The processing of an RSA cryptographic code is not an operation within a finite field.

As understood in the art, when generating an RSA cryptographic code key, a pair of prime numbers p and q are generated, then a value, for example, $n = p \times q$ is obtained for deriving e and d satisfying a relation, $ed = 1 \bmod (p-1) \times (q-1)$, wherein, (n, e) is a public key and (p, q, a) is a private key. When encrypting a massage in, and obtaining the associated

encryption message, called an encryption message c, m^e is subjected to an operation of mod n of which the result is 0. When decrypting the encryption message c, c^d is subjected to an operation of mod n. That is, a pair of numbers (n, e) is normally called an RSA key and the bit length of n is called the key length. n is a compound number and, hence, is not a prime number so that the operation of mod n is not an operation within a finite field.

That is, a teaching regarding a length of an RSA key does has nothing to do with the finite field expression associated as the Examiner contends.

Unsupported Taking of Official Notice

In rejecting dependent claims 3, 14, and 18, the Examiner contends that "keys are inherently developed using a random number generator, which would generate them automatically." (Action at page 6).

Applicant submits that such Examiner's contentions are unsupported taking of Official Notice, and the rejection should be withdrawn and claims 3, 14, and 18 allowed.

Conclusion

Since features of the claims are not taught by the cited art, alone or in combination, and *prima facie* obviousness is not established, and there is no motivation stated within the art to combine the art or reasonable chance of success if *arguendo* combined, the rejection should be withdrawn and claims allowed.

ITEM 4: REJECTION OF CLAIMS 4-5 and 13

Dependent claims 4-5, and 13 recite, for example, using claim 4 as an example an generating apparatus "wherein when the extension degree is inputted as the condition, said generation device automatically generates irreducible polynomial data corresponding to the extension degree and stores the irreducible polynomial data in said expression data storage device."

The Action concedes that Leppek does not teach generation of polynomial expressions. (Action at page 4). Nevertheless, the Examiner rejects dependent claims 4-5 and 13 under 35 U.S.C. §103(a) over Leppek in view of Wright. (Action at pages 4-5).

The Examiner contends the feature is taught by Wright and there is motivation to modify Leppek.

Applicant submits that the polynomial generated by randpoly in "Wright" has coefficients that are assigned in a random manner and hence it is different from an irreducible polynomial associated with the present invention

That is, Wright does not teach a random polynomial is generated and the generated polynomial is examined if it is irreducible. The process constituting the part for generating a random polynomial is a very popular process therefore it is no surprise to find the process representing the same function with that of randpoly.

Conclusion

Since features as recited by claims 4-5 and 13 are not taught by the cited art, alone or in combination and *prima facie* obviousness is not established, the rejection should be withdrawn and claims 4-5 and 13 allowed.

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

If there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: December 13, 2004

By: _____
Paul W. Bobowiec
Registration No. 47,431

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

CERTIFICATE OF FACSIMILE TRANSMISSION
I hereby certify that this correspondence is being transmitted via facsimile to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450
on December 13, 2004
STAAS & HALSEY
By: _____
Date December 13 2004